IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. I (Mar-Apr. 2014), PP 20-25
www.iosrjournals.org

Dynamic Router Selection and Encryption for Secure Data Transmission in Wireless Sensor Networks

Vyshak C, Aruna M G
Dept. of CS&E, M S Engineering College, Bengaluru-560064,Karnataka
Associate professor, Dept of CS&E, MSEC, Bengaluru-560064,Karnataka .

Abstract*: Among the various possible threats in the WSN's, like node failure, data security, etc., we are presenting this paper in order to circumvent or overcome the 'black holes' that are formed due to compromised -node (CN) and denial-of-service (Denial of service) by using some routing mechanisms. Basic idea of developing this paper is nothing but combat the vulnerability of existing system in handling such attacks due to their deterministic nature i.e., once an obstructionist can gather or acquire the routing algorithm can figure out the same routes known to the source, and hence intimidate all information sent over these routes. We have developed a structure that generates randomized routes. Under this design the routes taken by the "shares" of different packets change over time to time increasing the probability of randomness of paths to be selected for transferring the information. Therefore, even though adversary or offender comes to know about the routing algorithm still he cannot pinpoint the routes in where each packet is traversed randomly. Apart from randomness, the routes that are generated by our mechanisms are energy efficient as well as dispersive which ultimately make them capable of circumventing the black holes at less energy cost. Extensive frameworks are conducted to verify the validity of our mechanisms.*

Keywords*: Compromised Node (CN), Denial of service (DOS), and Wireless Sensor Networks (WSN), Purely Random Propagation (PRP).*

I. Introduction

Wireless communication is the transfer of information over a distance without the use of electrical conductors or cables. The distances involved may be short or long. Wireless operations permits services, such as long-range communications, that are impossible with the use of wires. Information is transferred in this manner over both short and long distances.

Sensor networks are the key to gathering the information needed by smart environments [1]. A sensor network is required in the present scenario that is fast and easy to install and maintain. The individual nodes that constitute a wireless sensor network are generally small in size and use power-efficient batteries to extend their operational longevity.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions to cooperatively pass their data through the network to a main location.

The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring, control, and machine health monitoring. The WSN is built of nodes from a few to several hundreds or even thousands, where in each node is connected to one (or sometimes several) sensors.

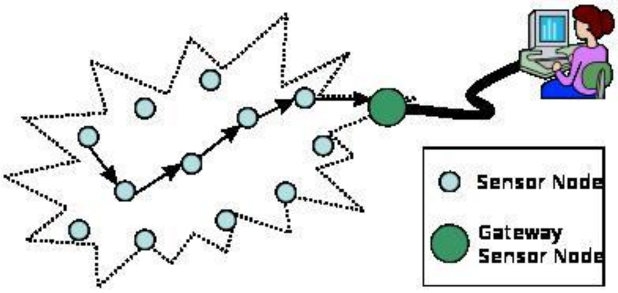

Figure 1.1: Typical multi-hop wireless sensor network architecture

Wireless sensor networks (WSN) will open the gates to the wireless revolution. But building a practical wireless network can be a daunting challenge unless the concepts are kept simple. In time, the new wireless technologies will likewise reshape society in unpredictable ways. A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the intensive efforts of person or persons to prevent an Internet site or service from functioning efficiently temporarily or indefinitely. A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services [3].

Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers. A DoS attack can be perpetrated in a number of ways. The five basic types of attack are[5]:

- Consumption of computational resources, such as bandwidth, disk space, or processor time.
- Disruption of configuration information, such as routing information.
- Disruption of state information, such as unsolicited resetting of TCP sessions.
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A. DoS attack may include execution of malware intended to:

- Maximum usage of processor , preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploit errors in the operating system, causing resource starvation thrashing available facilities so no real work can be accomplished.
- Crash the operating system itself.

B. Node compromise detection

It is a critical security requirement for the successful deployment of large-scale wireless sensor networks. A node compromise attack often consists of three stages:

i. The first stage is physically obtaining and compromising the sensors.
ii. The second stage is redeploying the compromised nodes back to the sensor network.
iii. The last stage is compromised sensors rejoining the network and launching attacks.

These two attacks are similar in the sense that they both generate black holes and the areas within which the opponent can either passively intercept or actively block information delivery. The objective of our study is to propose a randomized multi-path routing algorithm that can overcome the black holes formed by Compromised-node and denial-of-service attacks. Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically infeasible. Depending on the type of information available to a sensor, we have develop our distributed scheme for propagating information shares called Purely Random Propagation (PRP). PRP utilizes only one-hop neighborhood information and provides baseline performance. To diversify routes, an ideal random propagation algorithm would propagate shares as depressively as possible.

A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because once a node is compromised, the adversary can always acquire the secret keys of that node, and thus can intercept any information passed through it. At the same time, an rival can always perform certain form of DOS attack (e.g., jamming) even if it does not have any knowledge of the crypto-system used in the WSN. One solution to these attacks is to exploit the network's routing functionality. Specifically, if the locations of the black holes are known a priori, then data can be delivered over paths that bypass these holes, whenever possible. We argue that three security problems exist in the above counter attack approach:

- First, this approach is no longer valid if the adversary can selectively compromise or jam nodes. This is because the route computation in the above multipath routing algorithms is deterministic for a fixed topology, a fixed set of routes are always computed by the routing algorithm for given source and destination.

- Second, as pointed out in, actually very few node-disjoint routes can be found when node density is moderate and source and destination nodes are several hops apart. The lack of enough routes significantly undermines the security performance of this multipath approach.
- Third, even worse, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to avoid a moderate-sized black hole.

In this paper, we propose a randomized multipath routing algorithm that can overcome the above problems. In this algorithm, multiple paths are created in a randomized way whenever an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing time to time and a large number of routes can be potentially generated for each source and end. To intercept different packets, the opponent has to compromise or jam all possible routes from the source to the destination, which is practically impossible.

Because routes are now randomly generated, they may no longer be node-disjoint. However, the algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent constraint on energy consumption in WSNs, the main challenge in our design is to generate highly dispersive random routes at low energy cost. As explained later, such a challenge is not trivial. A naive algorithm of generating random routes, such as Wanderer scheme (a pure random-walk algorithm), only leads to long paths containing many hops, and therefore, consuming lots of energy without achieving good dispersiveness.

Due to Security considerations, we also require that the route computation be implemented in a distributed way, such that the final route represents the aggregate decision of all the nodes participating in the route selection. As a result, a small number of compromised nodes cannot dominate the selection result. In addition, for efficiency purposes, we also require that the randomized route selection algorithm only incurs a small amount of communication overhead.

II. Existing System

SPREAD algorithm in attempts to find multiple most-secure and node-disjoint paths. The security of a path is defined as the likelihood of node compromise along that path, and is labeled as the weight in path selection. A modified Dijkstra algorithm is used to iteratively find the top- K most secure node-disjoint paths. The H-SPREAD algorithm improves upon SPREAD by simultaneously accounting for both security and reliability requirements. Distributed Bound-Control and Lex-Control algorithms, which computes multiple paths, respectively, in such a way that the performance degradation (e.g., throughput loss) is minimized when a single-link attack or a multilink attack happens, respectively. Flooding is the most common randomized multi-path routing mechanism. As a result, every node in the network receives the packet and retransmits it once [5]. To reduce unnecessary retransmissions and improve energy efficiency, the Gossiping algorithm was proposed as a form of controlled flooding, whereby a node retransmits packets according to a pre-assigned probability. Parametric Gossiping was proposed to overcome the percolation behavior by relating a node’s retransmission probability to its hop count from either the destination or the source as shown in figure 1. A special form of Gossiping is the Wanderer algorithm, whereby a node retransmits the packet to one randomly picked neighbor. When used to counter compromised node attacks, flooding, Gossiping, and parametric Gossiping actually help the opponent to intercept the packet, because multiple copies of a secret transmission are dispersed to many nodes.

Disadvantages of Existing System:

- Existing randomized multi-path routing algorithms in WSNs have not been designed with security considerations in mind, largely due to their low energy efficiency.
- Multi-path routing mechanism, Gossiping algorithm has a percolation behavior, in that for a given retransmission probability, either very few nodes receive the packet, or almost all nodes receive it.
- The Wanderer algorithm has poor energy performance, because it results in long paths.

III. Proposed System

Our proposed solution is to establish a randomized multi- path routing algorithm that can overcome the black holes formed by Compromised-node and denial-of-service attacks. Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. To intercept different packets, the intruder has to compromise or jam all possible routes from the source to the destination, which is practically infeasible.

Advantages:

- Provides highly dispersive random routes at low energy cost without generating extra copies of secrete shares.
- If the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet
- Energy efficient

IV. Randomized Multipath Delivery

We consider a three-phase approach for secure information delivery in a WSN as illustrated in figure 2:

- Secret sharing of information,
- Randomized propagation of each information share, and
- Normal routing (e.g., min-hop routing) toward the sink.

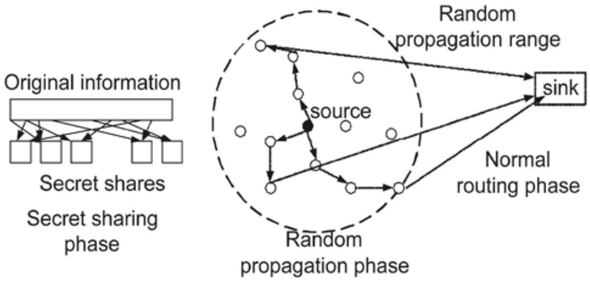

Figure 2: Randomized routing in WSN’s

More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares, according to a (T, M) -threshold secret sharing algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to other randomly selected neighbors, and so on. In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the TTL field is reduced by 1. When the TTL value reaches 0, the last node to receive this share begins to route it toward the sink using min-hop routing. Once the sink collects at least T shares, it can reconstruct the original packet. No information can be recovered from less than T shares.

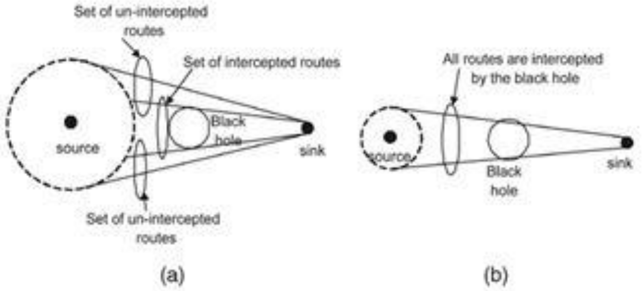
Set of un-intercepted routes
Set of intercepted routes
source
Black hole
sink
Set of un-intercepted routes
(a)
All routes are intercepted by the black hole
source
Black hole
sink
(b)

Figure 3: Implication of route depressiveness on bypassing the black hole.

(a) Routes of higher depressiveness. (b) Routes of lower dispersiveness.

The effect of route depressiveness on bypassing black holes is illustrated in Figure 3. A larger dotted circle implies that the resulting routes are geographically more dispersive. Comparing the two cases in Figure 3, it is clear that the routes of higher depressiveness are more capable of avoiding the black hole. Clearly, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism[6].

Random Propagation of Information Shares

To diversify routes, an ideal random propagation mechanism or algorithm that would propagate shares depressively as much as possible. Typically, this means propagating the shares farther from their source and towards the sink. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. Now the challenge here lies in the random and distributed nature of the propagation i.e. a share may be sent one hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from a security point of view. To tackle this issue, some control needs to be imposed on the random propagation process. Generally we have four types of schemes:

a. Purely Random Propagation (Baseline Scheme)
b. Non- repetitive Random Propagation
c. Directed Random Propagation
d. Multicast Tree-Assisted Random Propagation

The random routes generated by the four algorithms are not necessarily node disjoint. Note that the security analysis for the CN and DOS attacks is similar because both of them involve calculating the packet interception probability [5]. For brevity, we only focus on the CN attack model. The same treatment can be applied to the DOS attack with a straightforward modification. Basically this paper involves three important steps for implementing secure data transmission in WSN's using some programming language like java and database like ORACLE is as follows which include three modules:

A. Topology Creation

In this module, we construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and IP address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

B. Randomized Multipath Routing

We achieve randomized multipath routing that can conquer the Compromised Node attack & Denial of Service attack. Here several paths are computed in

randomized pattern each time an information packet needs to be sent. In this context a large number of routes can be potentially produce for each source and destination as shown in figure 4. To capture different packets, the offender need to compromise and squash all possible routes from the source to the destination, which is practically not possible.

C. Message Transmission

Pure Random Propagation (PRP): Shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all nodes within its transmission range. When a source node wants to send data to destination, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing.

Secured Delivery of Packets**:** In this module we can maintain the routing table; here we add one more column to maintain the packet delivery ratio. In this way we can maintain how many packets are transmitted over each path. It will be useful to identify any path and can packets handle packets number. We can stop transmission for some amount of time period over that path, so that the hacker cannot identify in which path the message is transmitted and also we can easily transmit the data securely.

V. Conclusion

This paper depicts the effectiveness of the randomized dispersive routing in overcoming the CN and DOS attacks which is energy efficient. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithms to a better extent. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Specifically, the energy consumption of the projected randomized multipath routing algorithms is only one to two times higher than that of their deterministic complement algorithms. The proposed algorithms can be applied to selective packets in WSNs to provide additional security levels against adversaries attempting to acquire these packets. Energy cost plays a key role in this proposed system where energy of a node is increased to an extent due to the reduction in unnecessary retransmissions which ultimately increases the battery life of a sensor node too. Our current work is based on the assumption that there is only a small number of black holes in the WSN. Because in reality a stronger attack could be formed whereby the offender selectively compromises a large number of sensors forming many black holes around the sink. The paper resolution requires us to extend our mechanisms further.

References

[1] G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[3] H. Poor, An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.

[4] B. Smith, “An approach to graphs of linear forms (Unpublished work style),” unpublished.

[5] E. H. Miller, “A note on reflector arrays (Periodical style—Accepted for publication),” IEEE Trans. Antennas Propagat., to be published.

[6] J. Wang, “Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication),” IEEE J. Quantum Electron., submitted for publication.